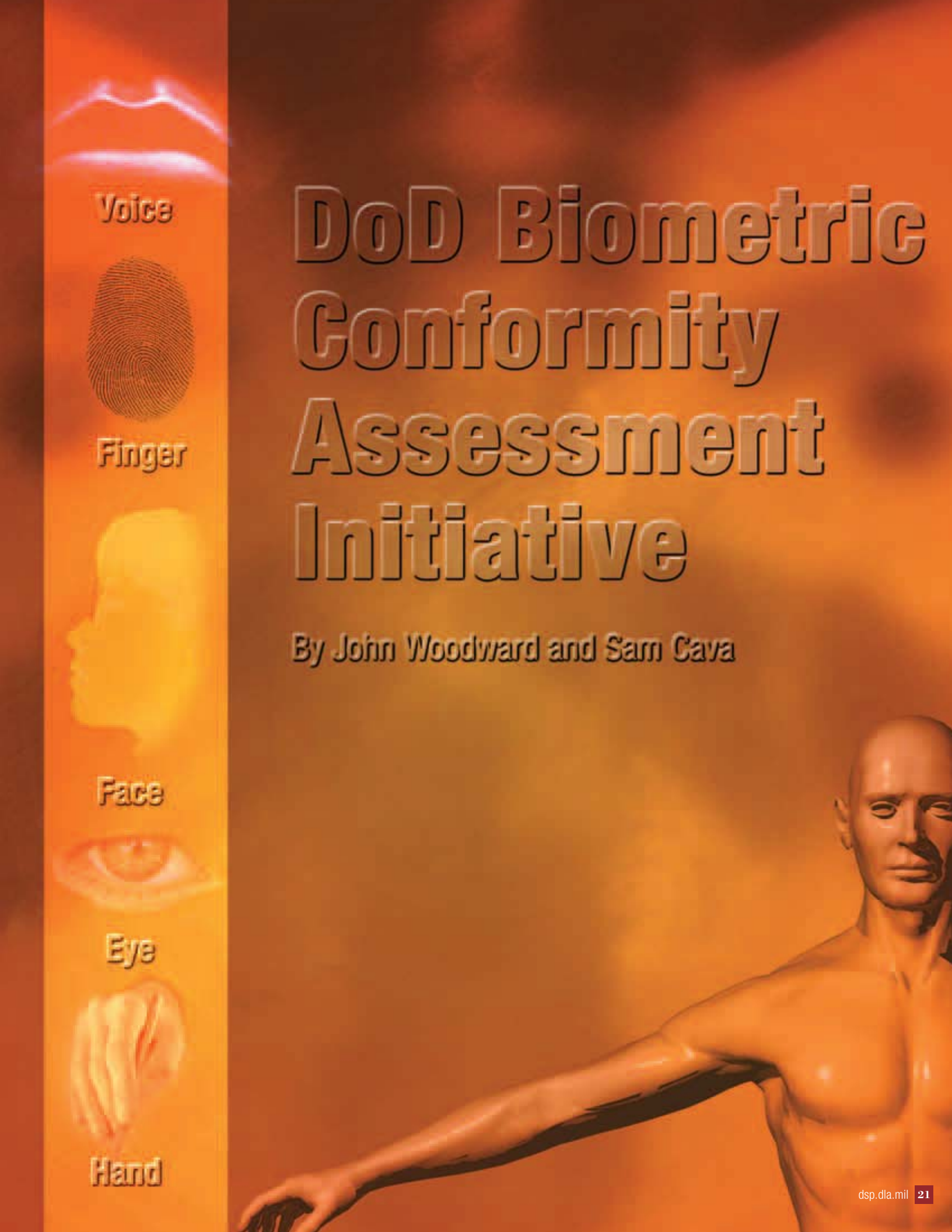

DoD Biometric Conformity Assessment Initiative

By John Woodward and Sam Cava

The comprehensive discipline of conformity assessment involves conformance testing activities and the certification of information systems to ensure that adopted standards are met. This article provides an overview of conformity assessment, and details the steps the DoD Biometrics Management Office (BMO) and its subordinate technology center, the DoD Biometrics Fusion Center (BFC), have underway to establish such a conformity assessment program for the implementation of interoperable biometric technologies. With such a program implemented, DoD components will adhere to DoD policies that emphasize the need for conformity assessment activities to ensure the interoperability of forces, equipment, and processes.

Interoperability and Conformance Testing

Achieving greater interoperability among forces, services, and components—human and technical—is a DoD priority. Advances in biometric technologies, combined with the growing needs for physical and information security and support for U.S. efforts in the global war on terrorism, have furthered the importance of the effort. The interoperability of products and systems relies heavily on the application of developed standards in the design and manufacture of system components, as well as in the testing and validation of these components, to provide evidence of interoperability before acquisition and deployment.

Conformance testing stems from the global standardization effort. The American National Standards Institute (ANSI) and its international counterparts, the International Organization for Standardization (ISO) and International Electrotechnical Commission, continue to develop numerous standards for a wide range of activities in a variety of industries and disciplines. By having products, programs, and processes meet these standards, DoD will achieve greater reliability, quality, and interoperability.

Benefits of Conformity Assessment for DoD Biometrics

A comprehensive conformity assessment program helps ensure that DoD's biometric products are interoperable. A conformity assessment program can do the following:

- Verify that biometric products have been developed or modified to meet the appropri-

DoD Policy Documents Affecting Conformity Assessment

Several DoD-wide policy documents include provisions that affect or imply that conformity assessment programs are required to adequately meet DoD testing requirements:

- DoD Directive 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, January 2002.
- DoD Instruction 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, June 2004.
- Chairman of the Joint Chiefs of Staff Instruction 6212.01C, *Interoperability and Supportability of Information Technology and National Security Systems*, November 2003.
- National Security Telecommunications and Information Systems Security Policy 11, *National Information Assurance Acquisition Policy*, revised July 2003.

ate ANSI or ISO standards mandated within DoD

- Determine whether considered biometric products have been sufficiently tested to meet the adopted standards
- Confirm that testing activities and test results are complete, reproducible, and verifiable
- Determine that the performance of testing facilities and instruments meets accepted industry standards
- Provide accreditation to testing laboratories that are performing properly to accepted, recognized national and/or international standards
- Determine the qualification of personnel who perform conformance testing
- Disseminate lists of properly tested and certified vendor products for DoD community consideration.

Steps Underway to Establish a Conformity Assessment Program

CONFORMANCE TESTING

Conformance testing ensures that standards adopted by a program are met. To enhance their credibility, product conformance testing procedures should follow well-designed testing methods that detail accuracy and variability requirements. Test methods alone are not sufficient tools for testing. Instead, test methods should be executed in the form of conformance test suites (CTSs), which are automated tools used to determine products' conformance to standards.

Three general approaches are used for conformance testing:

- First-party testing, which is performed by vendors on their own products. The primary risk associated with first-party testing is that consumers have less confidence in testing results because consumers do not control the testing process. The concern is that a potentially biased tester may influence the testing results.
- Second-party testing, which is performed by the consumer organization. The primary risks associated with second-party testing are that it may add cost and responsibility to the consumer organization. However, because the consumer has control over the product sample, testing environment, testing staff, and testing processes, the consumer has greater confidence that tested products will conform to approved standards. This allows the testing results to be more readily accepted.
- Third-party testing, which is conducted by a trusted testing laboratory independent of both producer and consumer groups. DoD views third-party testing as the least feasible option due to its primary risks—the time and higher costs it often requires. For example, if the testing of a specific version of product takes a significant amount of time, it is likely a newer version of the same product will be available before the older version is fully tested. This will place DoD (the consumer) in the position of having to choose either an approved older version of a product or a newer, but untested version of the product. The higher costs associated with third-party testing are typical in contracting agreements with third parties.

LABORATORY ACCREDITATION

Laboratory accreditation is granted by an authoritative body, which certifies that a laboratory is competent to perform testing. For example, if the National Institute of Standards and Technology (NIST) accredits a laboratory, the laboratory is recognized as being capable of certifying products through testing or other procedures. Laboratory accreditation is, of course, not a guarantee that the facility will competently test products at all times. It is for this reason

that independent verification and certification of test results are also recommended.

PRODUCT CERTIFICATION

Certification provides another level of assurance through independent verification and validation that a product conforms to a standard or specification or that an organization is competent to perform a certain task. As with conformance testing, there are three types of certification:

- First-party certification, which is implemented by a vendor to guarantee that its products meet one or more standards. Use and acceptance of a first-party certification system require a consumer to depend on a vendor's claims of conformity. The obvious risk is that a vendor may only partially conform to a standard while claiming to conform to that standard completely.
- Second-party certification, which is the use of the consumer's own certification authority to ensure that a desired product conforms to one or more standards. Test results may come from first-party, second-party, or third-party testing laboratories (as explained above), but the validation, verification, and certification activities are performed by the consumer's organization or certification authority.
- Third-party certification, which is the use of a technically and otherwise competent certification body—not controlled or influenced by the consumer or the vendor—to validate a product's conformity to one or more standards. As an example, NIST has accredited eight common criteria testing laboratories to perform test methods following Federal Information Processing Standards (FIPS) 140-1 and 140-2, *Security Requirements for Cryptographic Modules*. (For more information, see http://niap.nist.gov/cc-scheme/testing_labs.html and http://csrc.nist.gov/cryptval/.) These accredited laboratories act as third parties and validate that security products conform to FIPS 140-1 and 140-2. Credibility given to a certification from a third party generally depends on three factors: (1) the number and types of testing and inspection methods used to ensure product conformance, (2) the vendor's quality control system, and (3) the competence of the laboratory.

Approach to Implementing Conformity Assessment within DoD Biometrics

As illustrated in Figure 1, the BMO and BFC are key components of the proposed approach for implementing a conformity assessment program. Under this approach, the BFC is the testing laboratory that

Biometrics Management Office

The DoD BMO is responsible for leading, consolidating, and coordinating the development, adoption, and use of biometric technologies for the combatant commands, services, and agencies, to support the warfighter and enhance joint service interoperability. The BMO reports to the Army Chief Information Office, which acts on behalf of the DoD Executive Agent for Biometrics, the Secretary of the Army. The recently formed Identify Protection and Management Senior Coordinating Group provides senior-level, DoD-wide strategic guidance to the BMO, given its mission to oversee efforts in the areas of biometrics, public key infrastructure, and smart cards.

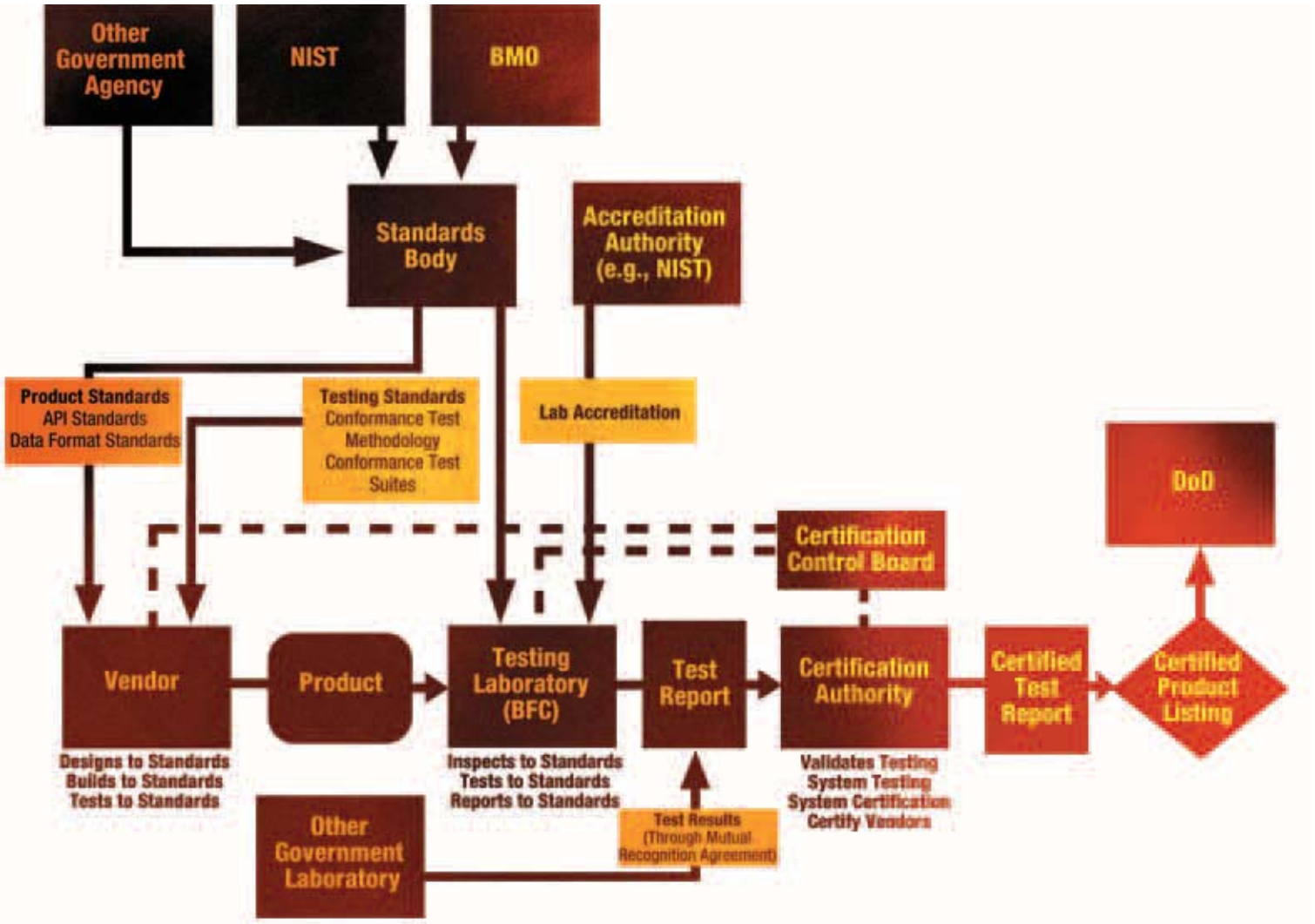

FIGURE 1. Proposed Conformity Assessment Approach.

determines the conformance of biometric technologies to relevant national and international biometric standards. To realize this approach, the BFC is working to establish itself as an accredited DoD biometric conformance testing laboratory. Once certified by an accreditation authority (e.g., NIST), the BFC will provide testing to determine whether vendors' products actually conform to biometric standards.

A certification authority will provide the necessary validation of the BFC's test results and the certification of products or technologies. The certification authority may also provide system testing when necessary to prove the interoperability of multiple technologies that have been combined into one system. Test reports and a list of certified biometric products will be made available to DoD through an appropriate interface.

The proposed conformity assessment approach also includes a certification control board—with representatives of the certification, testing, client, and vendor communities—that would provide a necessary interface between conformity assessment program components.

Under this proposed approach, the BMO (along with NIST and other government organizations) will continue to provide input to the development of product and testing standards for biometric technologies. These standards will be available to vendors and testing laboratories alike. Vendors of biometric tech-

nologies will be able to design, build, and self-test their products with respect to these standards.

Efforts in Motion

DEVELOP BIOMETRIC STANDARDS

Nearly every aspect of biometric technology must be standardized to ensure the interoperability and interchangeability of data, systems, and components. The BMO and BFC have begun work in this effort with acceptance of the Biometric Application Programming Interface (BioAPI) standard. Other standards, such as data interchange format standards for biometrics and DoD application profile standard, are being developed. These efforts are essential to the integration of biometric technologies for DoD. They are the building blocks of a solid conformity assessment program.

DEVELOP CONFORMANCE TEST STANDARDS

To ensure interoperability, and conformance of biometric products to national and international standards, standardized conformance testing methods must be developed and recognized. The BMO and BFC are currently working on several conformance testing methods in collaboration with national and international standards bodies. We are in the beginning stages of development, recognition, and subsequent implementation of the necessary standards for conformance testing of each related biometric technology.

DEVELOP CONFORMANCE TEST TOOLS

Conformance testing methods, in and of themselves, are not sufficient tools for testing. If testing organizations, such as BFC, are to perform the validation and verification of the biometric products, an executable CTS must be implemented. The BMO and BFC are working to identify existing tools. In addition, the BMO and BFC are developing tools that will implement the standardized conformance testing methods. For example, the BMO and BFC are developing a BioAPI CTS following the methods outlined in draft national and international BioAPI conformance testing standards. The goal of the BMO and BFC is to make conformance test tools—like the BioAPI CTS—publicly available. Vendors will then be able to determine if their products meet the selected standards.

Efforts for the Near Future

APPLY STANDARDS TO CONFORMANCE TESTING

With conformance testing methods and test suites appropriate to the specific technology involved, the BFC can incorporate full accountability and visibility into its objective and subjective testing methods, providing a higher degree of incontrovertible test results. It is well known that the cost of correcting mistakes increases as products move beyond research and development and into implementation phases. The greater use of recognized industry standards also allows DoD conformance testing to push the costs of faulty or non-interoperable biometric system components toward a preemptive, early error detection and correction phase. Vendors can concentrate more efficiently on development to meet the standards adopted by DoD. Testing and certification processes will move with greater ease and expediency.

ACCREDIT TESTING LABORATORIES

Testing laboratory accreditation, by a respected independent accreditation body, will provide the stamp of conformance to widely recognized laboratory standards to which the BFC should understandably be held accountable. This accreditation will give the BFC greater credibility with vendors and other testing laboratories. Accreditation is a necessary step toward obtaining the benefits that mutual recognition agreements provide.

Longer-Term Efforts

CREATE OR IDENTIFY A CERTIFICATION AUTHORITY

Having an independent certification authority verify and validate test results will provide added confidence

Biometrics Fusion Center

The DoD BFC is establishing itself as the biometric technology center of excellence for the DoD. The BFC tests and evaluates biometric products, supports the development of standards and performance measures, provides biometric repository support, and provides technical implementation and integration support to DoD organizations.

The BFC recently moved into a new facility in Clarksburg, WV, that significantly expands its capabilities. The BFC has a state-of-the-art demonstration center that highlights current and future biometric applications of interest to DoD. For more information, visit www.biometrics.dod.mil.

in the products and systems tested. The certification authority's attached certification control board will be able to resolve technical questions or disputes that may be related to the testing process. The certification authority is able to provide certificates of validation, conformance, and interoperability to products, systems, vendor quality systems, and personnel.

ESTABLISH MUTUAL RECOGNITION AGREEMENTS

Mutual recognition agreements (MRAs) allow accredited testing laboratories and product acceptance systems to recognize the testing results of other laboratories as being in conformance with applicable, recognized standards. This reduces the costs of testing and approval processes by eliminating redundant testing—testing that has already been completed by a competent laboratory whose findings DoD will recognize as valid. Establishing MRAs to recognize the certified results of other certification authorities outside of the direct DoD system is also possible.

Conclusion

With the open promotion and integration of recognized product and test standards, the accreditation of testing laboratories, and the implementation of accepted test validation and product certification by an independent agency, DoD will have greater confidence in the interoperability of biometric systems. Expediency and best efforts are required to protect facilities, people, and information and to address the relatively new challenges for identification and tracking in the global war on terrorism. A conformity assessment program established within DoD will help increase efficiency and accuracy of validation and verification of interoperability for biometric technologies, devices, and data. Tested and validated interoperability will provide logical security for DoD information systems; physical security on bases, mobile platforms, and other installations; and tracking of friendly personnel, as well as enemy combatants, common criminals, and potential terrorists—for now and in the future.

About the Authors

John Woodward is the director of the DoD Biometrics Management Office. Before joining the BMO, Mr. Woodward worked for the RAND Corporation under the authority of the Intergovernmental Personnel Act, which permits movement of personnel between qualifying organizations. At RAND, he served as a senior policy analyst.

Sam Cava is the director of the DoD Biometrics Fusion Center. He is responsible for enhancing the center's test and evaluation capabilities and establishing stronger ties with other DoD organizations and federal agencies. Mr. Cava came to the BFC from West Virginia University, where he was the director of Forensic and Biometric Development. Previously, he served on active duty with the U.S. Air Force, working in several intelligence-related assignments.